

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION**

CENTRIPETAL NETWORKS, INC.,

Plaintiff,

vs.

CISCO SYSTEMS, INC.,

Defendant.

Case No. 2:18-cv-00094-EWH-LRL

TRIAL BRIEF OF DEFENDANT CISCO SYSTEMS, INC.

Dabney J. Carr, IV, VSB No. 28679

TROUTMAN PEPPER

HAMILTON SANDERS LLP

P. O. Box 1122

Richmond, Virginia 23218-1122

Telephone: (804) 697-1200

Facsimile: (804) 697-1339

dabney.carr@troutman.com

Charles K. Seyfarth, VSB No. 44530

cseyfarth@ohaganmeyer.com

O'HAGAN MEYER

411 East Franklin Street, Suite 500

Richmond, Virginia 23219

Telephone: (804) 403-7137

Facsimile: (804) 237-0250

John M. Baird, VSB No. 77827

Christopher J. Tyson, VSB No. 81553

DUANE MORRIS, LLP

505 9th Street, N.W., Suite 1000

Washington, DC 20004-2166

Telephone: (202) 776 7851

Facsimile: (202) 478 2620

Louis N. Jameson (admitted *pro hac vice*)

Matthew C. Gaudet (admitted *pro hac vice*)

John R. Gibson, VSB No. 72968

Alice E. Snedeker (admitted *pro hac vice*)

DUANE MORRIS, LLP

1075 Peachtree Street, N.E., Suite 1700

Atlanta, Georgia 30309-3929

Telephone: (404) 253-6900

Facsimile: (404) 253-6901

Joseph A. Powers (admitted *pro hac vice*)

DUANE MORRIS, LLP

30 South 17th Street

Philadelphia, PA 19103-4196

Telephone: (215) 979-1000

Facsimile: (215) 689-3797

Counsel for Defendant Cisco Systems, Inc.

TABLE OF CONTENTS

| | | |
|-------|--|----|
| I. | Introduction..... | 1 |
| II. | Overview Of The Patent Process, As Background For The Disputes In This Case | 2 |
| III. | The State of the Art in Network Security When Centripetal Filed Its Applications | 3 |
| A. | Inline Security Devices | 3 |
| B. | Out-of-Band Monitoring | 5 |
| IV. | Overview Of Centripetal And Its Products..... | 6 |
| V. | Overview Of The Trial..... | 7 |
| VI. | The Disconnect Between Centripetal’s Four Patents And The Accused Products..... | 8 |
| A. | The ’193 Patent | 8 |
| 1. | The Requirements Of The ’193 Patent’s Claims | 9 |
| 2. | The Difference Between The ’193 Patent Claims And Cisco’s Products..... | 11 |
| B. | The ’176 Patent | 13 |
| 1. | The Requirements Of The ’176 Patent’s Claims | 13 |
| 2. | The Difference Between The ’176 Patent Claims And Cisco’s Products..... | 16 |
| C. | The ’856 Patent | 19 |
| 1. | The Requirements Of The ’856 Patent’s Claims | 19 |
| 2. | The Difference Between The ’856 Patent Claims And Cisco’s Products..... | 21 |
| D. | The ’806 Patent | 24 |
| 1. | The Requirements Of The ’806 Patent’s Claims | 24 |
| 2. | The Difference Between The ’806 Patent Claims And Cisco’s Products..... | 27 |
| VII. | Centripetal’s Willfulness Case Relies On Unsupportable Copying Allegations | 29 |
| VIII. | The Disconnect Between The Parties On Damages | 30 |

I. Introduction

Centripetal's case is based on a fundamentally incorrect premise about what the Patent Office did (and did not do) with Centripetal's patent applications. Centripetal proceeded at trial as if the Patent Office granted it patents that broadly cover basic concepts in the field of network security—concepts that are decades old. As is clear from the Patent Office proceedings and from the precise language of the claims themselves, the Patent Office repeatedly rejected Centripetal's efforts to obtain patents with broad coverage of well-established network security techniques. These rejections led to protracted negotiations with the Patent Office, during which Centripetal narrowed the scope of its requested patents by adding more and more limitations to its proposed claims. The addition of these increasingly specific requirements allowed Centripetal to distinguish its proposed claims from the prior art that the Patent Office identified, but the result was that Centripetal's patent claims have precise requirements that would only cover narrow, niche network security techniques—techniques that Cisco has never used.

At trial, Centripetal reversed course, ignoring the years of protracted negotiations with the Patent Office. Centripetal's trial strategy again sought to cover well-established network security concepts. In doing so, Centripetal glossed over the specific requirements of the asserted claims, even though those requirements were the only reason the Patent Office issued the patents.

To prevail in a patent case, the patentee must prove that the accused product satisfies every requirement (or limitation) of a patent claim. If even one requirement is not satisfied, there is no infringement. Here, multiple claim requirements are missing for each patent, and they are the very requirements Centripetal was forced to add to convince the Patent Office to issue the patents at all. Centripetal did not (and cannot) carry its burden of proving infringement.

This Trial Brief provides an overview of: (i) the patent application process; (ii) the network security technology at issue; (iii) the history of Cisco and Centripetal and their interactions; (iv)

the trial; and (v) the reasons why Cisco does not infringe these patents.

II. Overview Of The Patent Process, As Background For The Disputes In This Case

Patent Applications. When an inventor submits an application to the Patent Office, the application must include a description of the invention in a written specification. The specification usually includes a discussion of the technology that is already known, the problem the patent solves, and a detailed description of the invention.

Claims. The specification is followed by a set of proposed claims. A patent's claims appear at the end of the patent, and they define the metes and bounds of the invention. Each phrase in a claim is referred to as a requirement (or a synonymous term like "element" or "limitation"). Patent claims often include requirements based on what was already known, but must also add at least one new requirement. For example, the claim for an invention to monitor the pressure in a car's tire may read as follows:

An automobile including:
a dashboard;
a display on the dashboard that presents information to a driver;
a device for determining the pressure inside of each tire; and
software for presenting the amount of tire pressure on the display.

Every car for decades satisfies the first two requirements of this claim, but that is typical. This is because claims can include well-known requirements as long as the claim as a whole is novel and non-obvious. For this reason, every requirement matters when proving infringement. In this example, a car with a dashboard and a display does not infringe this claim unless it also has the last two requirements for determining the tire pressure and presenting it on the display.

Prosecution History. The Patent Office will examine the proposed claims to evaluate whether the claims are novel and non-obvious as of the "priority date" (35 U.S.C. §§ 102, 103). If not, the Patent Office will reject the claims. The priority date is usually the filing date of the original patent application. If the Patent Office rejects a claim, a back-and-forth negotiation can

occur in which a patentee might add more requirements to a claim, thus narrowing the scope of the patent. In the above example, if the Patent Office rejected the proposed claim because all of its requirements were already known in the prior art, then the patentee might add an additional requirement, such as the phrase *within one second of starting a car's engine* to the last requirement. If the Patent Office determines that this additional requirement distinguishes the invention from the prior art, it will issue the patent. Of course, the tradeoff for adding an additional requirement is that a car that does not satisfy it—here, displaying the tire pressure within one second—does not infringe. The process described above is known as the prosecution history, and it provides important guidance regarding what patent claims can and cannot cover.

III. The State of the Art in Network Security When Centripetal Filed Its Applications

To understand why Centripetal had to add so many requirements to its claims (and why, even then, so many of its patents were invalidated in IPRs), a description of the state of the art is helpful. Centripetal started filing patent applications in 2013. By then, the field of network security had been developing for several decades. For example, Cisco already had over 800 patents in the network security area. Trial Transcript (“Tr.”) 205:14-21. There were numerous well-known, decades-old approaches to network security. The two approaches discussed below are the most relevant to this case.

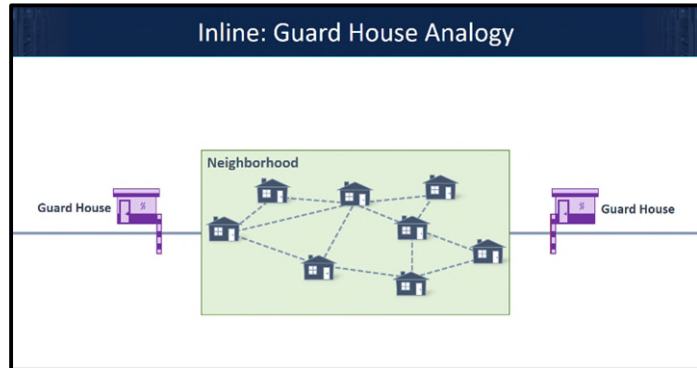
A. Inline Security Devices

Information travels over the Internet in the form of packets. Tr. 88:1-8. Any file (*e.g.*, an email) is broken into one or more **packets**, and then sent over the Internet to its destination. Tr. 98:12-25. Packets have two components: a **header** and a **payload**. Tr. 88:25-89:2. The header is like the information on the outside of an envelope (the sender’s address, the recipient’s address, and postage). The payload is like the letter inside the envelope. Packets are routed over the Internet and within local networks by devices called **routers** and **switches**. Tr. 108:7-21. Cisco invented

the router almost 50 years ago and remains the global leader.

Inline security devices stand “in the line” of the Internet traffic, receive and analyze each packet to determine if it might be dangerous, and if so, drop the packet before it can reach its target destination. Tr. 125:6-126:4. Below is an analogy for “inline” products. This image shows a neighborhood of houses (like a network of computers), which has 2 access roads (like Internet connections).

In this analogy, each of the roads is a path through which a thief (like malware) can enter and infect a protected area. The “inline” solution is to put a guard house (known as a **gateway** in a



computer network) at each of the entry points to the neighborhood. Tr. 118:13-120:12. A network gateway inspects packets using **rules** that the network administrator downloaded to the gateway, comparing each packet’s header to the rules in order to determine whether to drop or forward the packet. Tr. 119:11-120:12. Routers, switches, firewalls, and any other devices that sit inline can download rules to inspect packets. Tr. 2687:5-2688:5, 2549:24-2550:11.

This inspection of packets by comparing the header information with rules dates back to the beginning of the Internet. DTX-1687 at 27:19-28:8; Tr. 2549:24-2550:11. Then, in 2001, a company called Sourcefire (which Cisco acquired) released inline products known as “**firewalls**” that filtered packets in a more advanced way. DTX-1687 at 20:8-22:9; Tr. 2683:7-2689:12. Sourcefire’s products would check each packet against a set of 10,000 rules. PTX-134 at .0001-.0002 (referencing Sourcefire’s filtering of packets with “~10K rules”). In doing so, these products could analyze the header information, but could also look at a packet’s payload. Tr. 2685:25-2696:9 (Sourcefire’s SNORT rules “brings in the entire context of that packet, all the data that’s

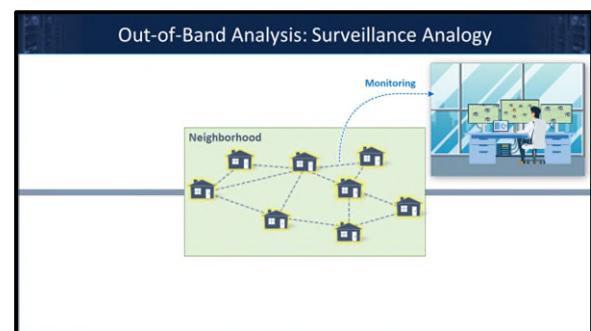
inside of it”). Like all approaches to security, the “inline” approach does not guarantee stopping every network security threat. Other approaches to network security complement inline filtering, such as “out-of-band” monitoring.

B. Out-of-Band Monitoring

In contrast to inline filtering, “out-of-band” monitoring is performed by devices that do not sit in the line of the traffic. Tr. 139:20-24. “Out-of-band” products analyze characteristics of packets that have already reached their destination. Tr. 133:16-134:2. This is done because computers may be infected without the user knowing, thus needing remediation.

For two decades, Cisco has sold out-of-band monitoring products based on a technology it invented called **NetFlow**. Tr. 136:5-18, 1760:23-1761:18, 2142:18-2143:12. A “**flow**” is a group of packets that all relate to a single communication session (*e.g.*, all of the packets sent as part of a video call, or an e-mail, might be a single flow). Tr. 107:13-108:4. NetFlow is a periodic **summary** of the flows that pass through network devices. Tr. 1672:1-1673:14. This summary can be sent to out-of-band products that a person (*i.e.*, network administrator) uses to analyze traffic that entered into the network. Tr. 137:2-138:16, 1672:1-1675:4. Using NetFlow, an administrator can evaluate whether a computer is infected and whether remedial action is needed. *Id.* Importantly, the underlying packets are not part of the NetFlow summary, and they are not sent to out-of-band monitoring products; only the summary NetFlow record is sent. *Id.*; Tr. 138:9-16. NetFlow became an industry standard in 2004 and is widely used. Tr. 136:5-18.

The analogy for out-of-band monitoring is that traffic has entered the neighborhood, and a security service is monitoring traffic from sensors to detect if a thief is in the neighborhood. Tr. 128:13-129:25, 131:19-133:15. Likewise, NetFlow



allows administrators to analyze traffic patterns indicating that a computer is infected. *Id.*; Tr. 137:2-138:16.

Most sophisticated networks have been using both inline and out-of-band approaches for decades. Both are used because no approach is perfect. Tr. 130:11-20, 139:20-140:12. Using different approaches together provides the strongest possible defense, while still achieving the goal of reliably delivering packets to and from user computers. *Id.* This is still true today.

IV. Overview Of Centripetal And Its Products

Centripetal was founded in 2009. In 2010, it acquired software and patents from a company called Great Wall. Great Wall created packet-filtering algorithms (*i.e.*, complicated formulas typically expressed in electronic form) that would allow an inline security device to use 5 *million* rules to evaluate packets, as opposed to the existing technology which used approximately 10,000 rules. In 2012, Centripetal started developing a product (called RuleGATE) with this technology, and its first sale was in December 2014. Centripetal also filed patent applications between 2013 and 2015, including those that led to the asserted patents.

Despite initial favorable press, Centripetal's 5-million-rule approach did not get traction in the marketplace. By 2015, Centripetal was soliciting investment from scores of security companies, including Cisco. This included outreaches to different Cisco employees in different groups, in hopes of finding a receptive audience. Tr. 1047:20-1049:4, 258:6-12; DTX-1690 at 18:21-21:10, 23:1-24:17(Akers). Cisco's Corporate Development team, which focuses on investments in startup companies and emerging technologies, entertained Centripetal's overtures. Although Cisco has invested over \$2B in hundreds of companies in the past 20 years, Tr. 2834:4-11, Cisco declined to invest in Centripetal. DTX-1374. Cisco concluded that its current approach relating to inline rules (using approximately 10,000 rules) was effective, and that any upside of

technology using 5 million rules for inline filtering was not worth the resulting false positives, delays in packet processing, and added costs. PTX-134. Importantly, Centripetal does not allege that Cisco ever used its 5-million-rules approach.

Centripetal sought strategic investments from dozens of network security companies and financial institutions, but none invested. Tr. 295:7-10, 1287:3-1290:8. Centripetal then turned to patent litigation as its main revenue source. It first sued Keysight, which settled mid-trial, and then it sued Keysight again in a dispute over the terms of its settlement. Centripetal next sued Cisco, both in this Court (in 2018) and in Germany (in 2020). In this Court, Centripetal originally asserted that Cisco copied and willfully infringed 11 patents, eight of which (including the '856 Patent) have since been invalidated by the Patent Office. In Germany, panels of three judges have found that Cisco does not infringe the foreign counterparts of the '806, '176 and '856 Patents. As to the final '193 Patent, Centripetal did not even present a case in Germany.

In 2021, Centripetal sued another major provider of security technology that also declined to invest: Palo Alto Networks ("PAN"). Remarkably, Centripetal's Complaint against PAN makes the same "willfulness" allegation, telling the same story: that Centripetal met with PAN to discuss a possible investment, PAN visited Centripetal's website, and then PAN instead copied Centripetal's patented technology. *PAN*, No. 2:21-cv-00137, Dkt. Nos. 1 at ¶¶ 50-60; 65 at ¶¶ 23-26 (E.D. Va.).

V. Overview Of The Trial

Centripetal's approach at trial was rhetorically clever, but legally flawed. Centripetal spent most of its time and effort on the claim requirements that were not really disputed, because they were part of most network security products long before Centripetal applied for its patents. But Centripetal had no evidence on the key claim requirements that were added as part of its protracted negotiations with the Patent Office. Using the exemplary claim above, this is like definitively

proving up the car, the dashboard, and the display, but not the crucial requirements for determining the tire pressure, *i.e.*, the requirements that had to be added for the patent to issue at all. Likewise, on the key requirements of its patents, Centripetal could only rely on distortions of statements made in Cisco's marketing documents, sometimes suggesting the products do things that would be impossible, all while contradicting (or ignoring) the source code and engineer testimony.

In contrast, Cisco provided testimony by the engineers who developed the accused products, including some who had written the source code or regularly worked with it, to explain how the accused products actually worked. Cisco's experts opined on the impossibility of Centripetal's infringement theories with respect to key claim requirements. The contrast between Centripetal's and Cisco's approaches to the key requirements will be fully explained below.

Finally, Cisco presented an invalidity case based on the principle that "if a claim term must be broadly interpreted to read on an accused device, then this same broad construction will read on the prior art." *01 Communique Lab., Inc. v. Citrix Sys., Inc.*, 889 F.3d 735, 742 (Fed. Cir. 2018). The purpose of Cisco's invalidity defense was to show that, if Centripetal glossed over key claim requirements when addressing infringement, then those broad accusations would apply equally to products that Cisco had been using for years before the patents. As the Federal Circuit explained, "when an accused product and the prior art are closely aligned, it takes exceptional linguistic dexterity to simultaneously establish infringement and evade invalidity." *Id.* at 742-43. If the Court agrees with Cisco that Centripetal failed to prove that the accused products satisfy every requirement of a given claim, then the Court need not reach invalidity. But if the Court finds that Cisco infringes a patent, that patent is invalid under *01 Communique*.

VI. The Disconnect Between Centripetal's Four Patents And The Accused Products

A. The '193 Patent

1. The Requirements Of The '193 Patent's Claims

The '193 Patent requires a specific *two-stage* filter for packets, but the evidence is clear that Cisco's products do not perform the critical *second* stage. Cisco therefore does not infringe.

Long before Centripetal filed the application for the '193 Patent, inline devices used tens of thousands of rules to filter packets. The '193 Patent covers a special type of rule that addresses a specific problem, known as "exfiltration." An exfiltration is when malware that is inside of a network sends sensitive information outside of the network. For example, malware might cause a computer inside of a law firm's network to send confidential information (*e.g.*, bank account information of clients) outside of the law firm (*e.g.*, to a hacker). The patent thus explains that exfiltrations involve the transfer of sensitive information (*e.g.*, "sensitive data or credentials" and "file transfers containing sensitive information") from a trusted network (*e.g.*, a law firm's network) to an untrusted network (*e.g.*, the Internet). JTX-4 at 1:24-27, 2:50-54.

The patent acknowledges that a great deal was known about exfiltrations by 2013. This included the specific protocols (and the computer commands for those protocols) that hackers used for exfiltrations: "many exfiltrations are facilitated by using popular network data transfer protocols, such as ... HTTP" and "attackers ... often use HTTP PUT or POST methods to exfiltrate sensitive data." *Id.* at 1:24-32, 7:18-19. The amount already known is confirmed by the length of the '193 claims, which include numerous requirements that the Patent Office made Centripetal add before agreeing to issue the patent. Claim 18, for example, goes on for 36 lines.

The '193 Patent's claimed solution to exfiltrations requires rules that filter (*i.e.*, decide whether to block) packets based on two different stages:

- First, the rules determine the *origin and destination* of the packets (where the packets came from and where they are going). The claims recite this requirement as "receive, from ... a first network ... a first portion of packets" and "wherein the data indicates that the first portion of packets is destined for the second network." *Id.* at 14:5-15.

- Second, the rules determine the “particular type of data transfer.” This focuses on the types of communications most likely to be exfiltrations. The claims recite this requirement as an “operator, specified by the ... rule” that is “configured to drop packets associated with the particular type of data transfer.” *Id.* at 14:16-19.

Centripetal’s claimed invention requires that the result of the rules (*i.e.*, the decision whether to block a packet) depends on the outcome at both stages. The specification explained why both stages are important to the blocking decision, and that the solution was not to simply filter packets based on the first stage. In fact, the first stage—applying rules to the origin and destination information in the packet header (*e.g.*, the packet’s internal network source address and external network destination address)—has been done for decades. The specification explains the problem with applying only the first stage: “While enterprise X could simply block all communications to networks it does not fully trust, this would likely result in enterprise X blocking access to most of the Internet.” *Id.* at 7:26-29. Centripetal’s CTO (Sean Moore) said the same thing in a declaration in support of Centripetal’s response to an *ex parte* reexamination: “prior attempts by others to prevent data exfiltration were often too coarse or overbroad because they would simply block *all* traffic *to/from a given network*, regardless of the actual threat.” Ex. 2028 to Centripetal’s 1-25-2021 Response in ’193 Re-exam at ¶ 11.¹

The ’193 Patent therefore requires a second stage: after the patent determines the origin and source of a packet based on the packet header (the first stage), the patent then applies “one or more additional operators” to determine the packet’s “*particular type* of data transfer.” JTX-4 at 2:19-29, 2:35-54, 8:39-65; DTX-369 at .007, .018, .021. Centripetal repeatedly relied on this second stage of filtering (*i.e.*, blocking the subset of packets that use “a particular type of data

¹ Centripetal created and submitted this document to the Patent Office after the conclusion of the trial. It is the subject of Cisco’s pending Motion to Supplement the Record. (Dkt. 691, 692-2).

transfer”) to save its patent from invalidation.

After Centripetal filed this lawsuit, Cisco asked the Patent Office to review the validity of this patent through an *inter partes* review (“IPR”). To convince the Patent Office not to institute that IPR, Centripetal argued to the Patent Office that the ’193 Patent claims have very specific requirements that distinguish its claims from otherwise invalidating prior art:

[T]he independent claims of the ’193 Patent recite rules for preventing the transfer of a subset of packets on the network. These rules involve a two-stage process for filtering traffic . . . In this manner, dangerous exfiltrations can be prevented on the basis of (1) detecting communications between two identified resources (*i.e.*, a first network and a second network, as claimed), and (2) using an operator to determine whether the rule allows for the “particular type of data transfer.”

DTX-369 at .007. In this same filing, Centripetal confirmed its argument: “**responsive to**” the “determination” of the first stage—the second stage asks a further question and only drops the subset of the packets that are also associated with “the particular type of data transfer.” *Id.* at .018. And Centripetal left no doubt in explaining that its invention required more than just blocking based on the packet’s source and destination in the first stage, but “also introduced the concept of applying an operator that can determine whether the packet is associated with a particular type of data transfer. . . .” *Id.* at .021.² Those “statements made by a patent owner during an IPR proceeding” are now binding on Centripetal. *Aylus Networks, Inc. v. Apple Inc.*, 856 F.3d 1353, 1359-62 (Fed. Cir. 2017).

2. The Difference Between The ’193 Patent Claims And Cisco’s Products

² This document includes many more pages in which Centripetal repeated this same point multiple times, providing confirmation of this fundamental two-stage requirement. As explained in Cisco’s pending Motion to Supplement the Record (Dkt. 691, 692-3), the parties presented Judge Morgan with trial notebooks that included all pages of an exhibit, but he ordered that only pages specifically referenced at trial be entered into the record. While those pages are more than sufficient to establish the critical point, Cisco seeks to provide the entirety of the document for the Court to review (in the form it was available to Judge Morgan) as a matter of completeness.

Centripetal alleges that Cisco's routers and switches, working with a Cisco management device called the Identity Services Engine (or "ISE"), infringe the '193 Patent because the routers and switches can implement "**quarantine**" rules (also referred to as quarantine Security Group Access Control Lists ("SGACL")) issued by ISE. Routers and switches implement these quarantine rules to filter packets coming from any computers that the ISE device has assigned to the list of users to be quarantined. Tr. 2379:2-2383:10, 2390:16-2391:15.³ Centripetal did not accuse any other product or rules of infringing this patent. Tr. 791:14-792:24, 2377:13-2379:1.

A quarantine rule can isolate a user's computer after the computer has been infected, just as a person with an infectious disease might be quarantined. The accused quarantine rules are only based on the source and destination of the packets, which is the first stage of the '193 claims—but there is no second stage. The quarantine rules thus restrict a given source computer from sending *anything* to an unpermitted destination. This approach is what Centripetal's CTO declared to the Patent Office is "too coarse or overbroad," in contrast to the solution of the '193 Patent. Cisco's expert explained that the quarantine rules' decision to drop a packet is not based on the "particular type of data transfer," and so does not practice the critical second stage:

Q. Dr. Crovella, let's get to the punch line. Is a quarantine rule a two-stage process?

A. No.

Q. Why not?

A. A quarantine rule looks only at the question that's being asked in the green portion of this slide. It's only asking about the -- where the packet's coming from and where it's going. The quarantine rule does not ask whether the packet is part of a particular type of data transfer.

Tr. 2377:2-10. Centripetal's expert (Dr. Mitzenmacher) confirmed this same dispositive point:

³ More specifically, administrators (humans) use the ISE management device to (i) assign a given user's computer to a given "security group", and to (ii) create rules for each "security group" that defines what access the computers in that group have to other devices in the network and to external networks. Tr. 2390:16-2392:2, 2388:21-2389:19. A quarantine rule is one such rule that ISE can download to a router or switch. *Id.*; Tr. 2265:5-2266:12.

So the way typically the policies are instrumented is you restrict according to source and destination. So you would say, well, I'm not going to let you reach out to this other location, to this other network, right, and it will block sort of that -- it will block the communication between you and that other network.

Tr. 528:3-8. He likewise acknowledged that the accused quarantine rules decide to “deny” or “permit” a packet based on the packet’s source and destination information found in the header. *Id.* at 869:8-12; 545:25-546:12.

Remarkably, Centripetal’s infringement expert never addressed Centripetal’s statements to the Patent Office in the IPR proceedings regarding the second stage—likely because this was the critical requirement Centripetal could not prove. As a result, the first witness who addressed the IPR and the requirement of the second stage was Cisco’s non-infringement expert, Dr. Crovella. He testified that this second stage requirement was exactly what Centripetal relied on to convince the Patent Office not to institute an IPR on this patent. Tr. 2375:1-2376:4. When he started discussing the first stage and second stage requirements, Tr. 2370:12-2372:25, Centripetal objected that “[t]his has nothing to do with the claims for the ’193 patent,” Tr. 2373:1-5, even insisting that it was misleading to suggest that the ’193 Patent requires two separate stages. Tr. 2373:6-2374:21. It was Centripetal that misled the Court and was wrong.

B. The ’176 Patent

1. The Requirements Of The ’176 Patent’s Claims

The ’176 Patent addressed the problem that packets could be “obscured” as they passed through a network device. Imagine, for example, a movie scene in which a villain tries to escape the police by running into a tunnel wearing one outfit, but then comes out of the other end of the tunnel disguised in a different outfit. Likewise, it is possible that packets can be disguised as they pass through network devices (such as routers and switches), effectively disguising the relationship between (i) the packets going into the network device and (ii) the packets coming out of the

network device, making it difficult to track where the packets originated. Centripetal believed that it could identify the disguised packets by “correlating” the characteristics of packets going into the network device with the characteristics of packets coming out of the network device, and thereby determine which packets matched and from where they came.

Two background points assist in understanding this problem and the claimed solution.

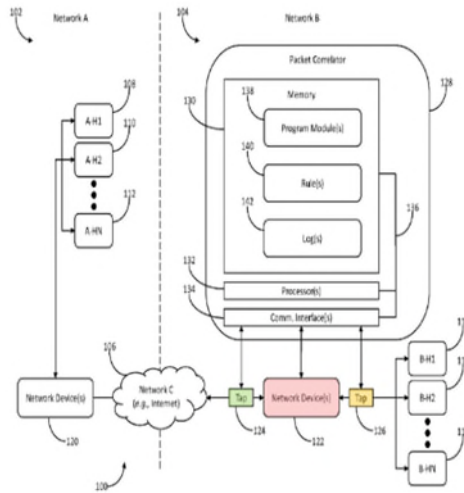
First, packets can generally be grouped together into “flows,” as noted above. The patent explains this basic principle: “the packets received by network device may be associated with one or more flows, (*e.g.*, distinct end-to-end communications sessions)” JTX-3 at 1:51-53. All of the packets in a flow will have some common identifying characteristics in their headers, which will allow devices to identify packets as being part of the same flow.

Second, some “network devices” (*e.g.*, a gateway to a network) might change some aspect of a packet’s header as the packet passes through the network device (like in the villain analogy). For example, a gateway might change the source address in the packet’s header. As a result, the next device that receives the packet cannot determine the true source of the packet. This can be a problem, *e.g.*, if that next device has a packet filter and is unable to determine the flow to which the packet belongs because it cannot determine the packet’s true source.

The solution was to “correlate” (i) information about packets that enter into a network device (such as a router or switch) with (ii) information about the packets as they exit the same device. This correlation would allow the system to detect that an exiting packet must have been modified, then uncover the disguise (by matching the modified packet to the unmodified packet), and then use information from the unmodified packet to identify the source of the exiting packet.

The patent specification teaches how this works. In Figure 1 (reproduced below with highlighting), the patent shows a “network device,” highlighted in red. The network device could

be a gateway that controls access into the network. On either side of the network device, there are separate devices called “taps” (highlighted in green and orange), which the patent explains are packet filtering devices running rules. *Id.* at 3:23-25. Those “taps” could be devices that use rules to filter traffic (*e.g.*, a Centripetal RuleGATE could be the green tap). *Id.* The network device (in red) might obscure the ability of the filter (in the tap) to associate packets with their flows: “the network device may alter the packets in a way that obscures their association with the flow(s) from the computing system.” *Id.* at 1:53-56. A filter located after the network device (*e.g.*, the tap) thus cannot tell which packets were associated with which flows and from where they originated.



The patent’s solution was to use taps on each side of the network device for “[c]orrelating the packets transmitted by the network device with the packets received by the network device [to] enable the computing system to determine the packets transmitted by the network device are associated with the flow(s).” *Id.* at 1:56-60. If the network device had obscured the packet’s identity, the correlation analysis would search for common characteristics between the ingoing/outgoing packets to determine that the two packets are actually modified versions of each other, and thus they originate from the same source. *Id.* at 8:64-9:43. The ’176 claims then require that the system use this correlation to generate rules to filter packets from that source.

The ’176 claims have many requirements. Claim 11, for example, covers 30 lines, and it has a series of specific correlation requirements. The mere fact that a security system does some form of “correlating” between different kinds of information is not enough for infringement.

Instead, the claims require that two specific things be correlated: (1) packets *received by a network device* (*i.e.*, packets entering a device) with (2) packets *transmitted by that same network device* (*i.e.*, packets exiting that device). The below portion of the claims spells this out:

identify a plurality of **packets received by a network device** from a host located in a first network;

generate a plurality of **log entries** corresponding to the plurality of packets received by the network device;

identify a plurality of **packets transmitted by the network device** to a host located in a second network;

generate a plurality of **log entries** corresponding to the plurality of packets transmitted by the network device;

correlate, based on the plurality of log entries corresponding to the plurality of packets received by the network device **and the plurality of log entries** corresponding to the plurality of packets transmitted by the network device, **the plurality of packets transmitted by the network device with the plurality of packets received by the network device**; and

Id. at 17:19-25 and 19:7-14. The orange elements require logging packets received by the network device (received packets); the green elements require logging packets transmitted by that same device (transmitted packets); and the purple elements require determining the correlation between the two sets of packets based on the two sets of logs.

2. The Difference Between The '176 Patent Claims And Cisco's Products

Centripetal accuses each individual Cisco router or switch as being a “network device,” but only when it is combined with an out-of-band product called **Stealthwatch**. Tr. 975:17-21. Routers and switches send NetFlow summaries to Stealthwatch, and so NetFlow is one source of information Stealthwatch can use to detect malicious activity and raise alerts. Stealthwatch also analyzes threat intelligence provided by third parties about possible data threats. Stealthwatch can use machine learning functionality called **Cognitive Threat Analytics (“CTA”)** for additional analysis. A network administrator (a human) can use Stealthwatch to monitor network traffic and

then make decisions whether to take action. Tr. 1674:12-25, 2143:2-9, 2146:22-2147:11.

The parties agree that every Cisco router or switch can create NetFlow records both for (i) packets *received* by the device (ingress records) and (ii) packets *transmitted* by the device (egress records). Tr. 978:1-10; 2250:8-13. The parties also agree that routers and switches send *some* of these NetFlow records to Stealthwatch (*e.g.*, every 30 seconds or longer, a switch or router sends Stealthwatch a NetFlow record that summarizes the flows of packets that traverse it). Tr. 2180:15-2181:3, 2248:12-2249:15. Finally, the parties agree that Stealthwatch (with CTA) performs analyses on flow summaries and presents the results to a human network administrator, who can take action. Tr. 2262:1-8. That is where the agreements end.

Tellingly, the patent does not discuss NetFlow, despite NetFlow being an industry standard since 2004. Tr. 2161:14-2162:9, 2334:9-12. Nonetheless, Centripetal accuses (i) NetFlow ingress records created by a router or switch as being the claimed “log entries” of packets *received* by the “network device”, and (ii) NetFlow egress records from that same router or switch as being the claimed “log entries” of packets *transmitted* by the network device. Tr. 977:13-978:10, 983:10-984:13. Critically, Centripetal’s infringement expert, Dr. Cole, then opined that Stealthwatch (specifically CTA) “correlates” (i) the NetFlow ingress records from a switch or router with (ii) the NetFlow egress records from the same router or switch, to satisfy the claims. Tr. 977:13-978:10, 1107:23-1108:10. He was wrong as a matter of fact.

Simply put, the evidence on which Dr. Cole relied does not support his opinion. He did not point to any specific source code on this element. Tr. 2254:16-18 (“Q. ... do you recall Dr. Cole presenting any source code evidence for the correlation limitation? A. He did not.”) This is because Cisco’s source code, technical documents, engineers, and expert witness all showed that Stealthwatch and CTA never correlate NetFlow ingress records (*i.e.*, records regarding flows going

into a router or switch or group of routers, or switches) with NetFlow egress records (*i.e.*, records regarding flows going out of that same router or switch, or group of routers or switches). Tr. 2180:15-2182:25, 2253:11-2254:15; PTX-569 at 39282. Instead, a NetFlow-based system like Stealthwatch is the opposite of the correlation-based system of the '176 Patent. When a Cisco switch or router generates a NetFlow record, the switch or router itself (as opposed to some other device) sends either the NetFlow ingress record or the NetFlow egress record to Stealthwatch. The router or switch only needs one NetFlow record (either the ingress record or the egress record) to understand the source of the flow. Sending both to Stealthwatch would be duplicative, and thus considered an “error” by the system. *Id.* In contrast, the '176 Patent is based on a system in which the relationship of packets entering a network device to the packets leaving it is unknown, which is what makes the packet correlation necessary. Tr. 2219:23-2222:6.

The reason the term “NetFlow” (or the generic term “telemetry,” which describes information summarizing a flow) never appears in the patent is because the invention has nothing to do with NetFlow. A NetFlow record identifies a flow. If a system uses a flow-reporting mechanism like NetFlow, the flow is not obscured—and so there is no need for the correlation solution of the '176 Patent. Former Centripetal employee Doug DiSabello, the product manager for RuleGATE, confirmed this:

Q. From your time at Centripetal and your work with the other inventors, were you ever aware of any solution that or any invention that applied analysis to logs or other NetFlow to detect cyber security threats?

A. No, not during my time there.

* * * * *

Q. So that concept of taking NetFlow from multiple observation points in a packet session, packets going into a network device, packets coming out of a network device, the idea of taking NetFlow or telemetry from those observation points and then correlating those packet flows together for analysis, it's not your understanding that Centripetal invented that, correct?

A. From my understanding, that's correct.

DTX-1685, DiSabello Dep. Tr. (Nov. 22, 2019) 142:8-142:13, 163:21-164:4.

To make up for this gap, Centripetal cited to virtually any Cisco document that used the word “correlate,” even though the word was used in entirely different contexts than the patent’s requirements. Tr. 2255:5-2258:23 (Cisco’s expert discussing Centripetal’s misplaced reliance on the word “correlation”). In taking this approach, Centripetal ignored the key requirement of the claims: logs of “packets received by a network device” must be correlated with logs of “packets transmitted by the network device.” Cisco’s products never do this.⁴

C. The ’856 Patent

1. The Requirements Of The ’856 Patent’s Claims

The asserted claims of the ’856 Patent stand invalid based on the May 23 FWD. Dkt. 686-1. As issued, the patent covered a special type of filtering used for “encrypted” packets. The use of encryption to protect information in the payloads of packets is decades old. An encrypted packet has had its payload locked, so that the payload cannot be viewed without the proper software “key” to unlock it. Former Centripetal employee Haig Coulter explained encryption as follows:

[I]f you think about a packet, it’s a lot like an envelope. There’s a to and a from. Sometimes the contents of that package are difficult to see because they’re encrypted. So you can imagine a postcard going through the mail where you can see what’s written on the postcard versus something in an envelope where you know where it’s from and who it’s to, but you can’t break into that envelope to see what’s inside.

DTX-1687 at 19:11-19. As in this analogy, even though the packet’s payload is encrypted (like the letter in the envelope), a packet’s header information must always be unencrypted (and thus fully visible, just like the outside of the envelope)—otherwise, network devices would have no

⁴ There is an additional, independent failure in Centripetal’s case. The claims also require that the accused “**system**” has to “generate” a “rule” based on the correlated packets. JTX-3 at 17:26-35, 19:14-23. The only rule generation Centripetal has identified in Cisco’s products does not spring from the accused “system,” but instead comes from humans being alerted of a possible network threat, Tr. 2266:5-2267:19, and then manually creating rules themselves.

idea where to send the packet. Technologies have long existed that use information from the unencrypted portion of packets (the header) to detect potential threats in packets whose payloads were encrypted, without decrypting the payloads. For example, Mr. Coulter confirmed that Sourcefire (where he worked before hired by Centripetal) and others used the unencrypted portion of an encrypted message to evaluate potential network threats for decades:

Q. Okay. Now, if the solution is to only look at the unencrypted portion of a encrypted message, could that also sit in the wire?

THE WITNESS: Yes.

Q. And that was also something that was happening in the 2010 timeframe by Sourcefire?

A. Yes.

THE WITNESS: Yes, and many other companies. Routers, fire -- firewalls are routers with rules and they are doing enforcement based on the unencrypted packet information and we have had firewalls for decades.

DTX-1687 at 27:19-28:8. Cisco witnesses said the same thing. *See, e.g.*, Tr. 1748:17-1749:7.

Against this backdrop, in December 2015, Centripetal sought a patent on the well-known concept of determining whether encrypted packets might be threatening by analyzing the unencrypted information in other packets in the flow. DTX-3 at 6163-64. For example, a given flow of packets might have both encrypted and unencrypted packets, and Centripetal originally proposed claims to cover the basic concept of determining whether the encrypted packets in the flow are malicious by analyzing the unencrypted packets in the same flow. *Id.* The Patent Office rejected those claims because that concept was already known in the prior art. *Id.* at 5072-75. Centripetal eventually convinced the Patent Office to issue the patent by more than doubling the number of requirements in the claims. DTX-3 at 4824-30, 4781-94. In May 2023, the Patent Office found the claims are not valid even with these additional requirements. Dkt. 686-1.

The claim language that Centripetal had added requires the following: if the computer performing the analysis on the packets determines that those packets have data “corresponding to

the one or more network-threat indicators,” then those *same* packets must be subject to a “filter.” Specifically, Claims 24 and 25 of the ’856 Patent describe the “filtering” of packets in a network through a specific multi-step process in the following order: the system must (1) “*identify . . . packets*” that have unencrypted data and encrypted data; (2) “*determine ... packets* comprising encrypted data that corresponds to the one or more network-threat indicators”; (3) “*filter ... the determined packets* comprising the encrypted data”; and (4) “*route ... filtered packets* to a proxy system.” JTX-5 28:59-30:31. The requirement that the *same* packets that are determined to correspond to network threats must also be the ones that are subject to this “filter” is dictated by the antecedent basis structure of the claim. When a patent claim uses the article “the” before a noun, it is necessarily referring to an earlier (antecedent) use of the same noun. *Wi-Lan, Inc. v. Apple, Inc.*, 811 F.3d 455, 462 (Fed. Cir. 2016). As a result, only an inline product (*i.e.*, a network device that receives packets and makes filtering determinations on the same packets) could infringe these claims.

2. The Difference Between The ’856 Patent Claims And Cisco’s Products

Centripetal accuses out-of-band devices that cannot physically do what the claims require. Centripetal accuses a combination of three separate devices that it alleges, if used together, infringe the claims. This combination is (1) a router or switch; plus (2) an out-of-band product called the **Identity Services Engine (“ISE”)**; plus (3) Stealthwatch (another out-of-band product) when used with a technology called “**Encrypted Threat Analytics (“ETA”)**).

Centripetal built its infringement case around ETA, even accusing Cisco of copying ETA from Centripetal. Yet, ETA is based on technology Cisco developed on its own. Tr. 1759:7-1773:22. ETA uses two new categories of information added to NetFlow records, which are sent by routers and switches to Stealthwatch. Working with CTA (described above), ETA uses the

artificial intelligence (“AI”) of CTA to determine if the packet flows summarized by NetFlow were likely malicious, even if encrypted. Tr. 1692:3-1693:25, 1749:18-1751:6. ETA is very much based on the use of AI algorithms. Tr. 1694:6-1695:23, 1749:18-1751:6.

In contrast to the essence of ETA, the ’856 Patent never references or relates to artificial intelligence, as confirmed by Mr. DiSabello, who is a named inventor on this patent:

Q. Okay. And you and the other inventors when you were working on this, you didn’t discuss doing any kind of threat detection packet by packet using statistical analysis or machine learning or artificial intelligence or any of that other kind of behavioral analytics, fair?

A. I did not, no.

Q. And are you aware of that from any of your co-inventors?

A. No. I mean, high level discussions of how else can we use machine learning, but not specific to this that I was aware of.

DTX-1685 at 141:10-21; *see also id.* at 128:9-18.

At trial, Centripetal tried to create an infringement case based on the broad similarity that (i) ETA relates to detecting threats in encrypted flows without having to decrypt the payloads of the underlying packets and (ii) the claims require (among other things) determining that an encrypted packet may be threatening without having to decrypt the payloads of the packets. But that broad similarity also exists with products going back decades, as Centripetal’s Mr. Coulter and others testified. For this reason, the Patent Office confirmed in the original prosecution that Centripetal did not invent this age-old concept of filtering encrypted packets without decrypting them—the precise reason why Centripetal had to add so many other requirements to its claims.

Against this backdrop, Centripetal’s infringement expert, Dr. Cole, offered an infringement theory that was impossible. He opined that the analysis of the packets (*i.e.*, the step in the claims where the system must “determine” if the packets correspond to a network threat) is performed by the ETA functionality in Stealthwatch analyzing NetFlow. Tr. 1081:25-1082:9, 1091:2-14 (discussing PTX-570 at 637-40). He further stated that Stealthwatch is also the required “filter” of

the packets. Tr. 1081:25-1082:15. This theory fails for several reasons.

First, the claims require acting on “packets”—*i.e.*, determining if “packets comprising encrypted data” meet certain network threat criteria, then “filter[ing]” those same packets, and then, under some circumstances, sending those “filtered...packets” to a proxy system. The Court’s claim construction ruling confirmed that the term “packets” has its ordinary meaning, Dkt. 202 at 22, which the parties’ experts agreed is a unit of data containing two different parts: the header and the payload, with the payload sometimes being encrypted. Tr. 26:23-29:16, 88:24-89:2. But Stealthwatch (of which ETA functionality is a part) is an out-of-band device that only receives and analyzes NetFlow records, which are summaries of entire packet flows; the “packets” themselves are never sent to Stealthwatch. Tr. 1672:19-1676:2 (Scheck), 2207:5-24 (Llewallyn). Stealthwatch simply cannot analyze the claimed “packets,” so there can be no infringement. Mr. DiSabello, a named inventor on the ’856 Patent, confirmed the difference between (i) the ’856 invention of analyzing, filtering and routing “packets” on an inline basis versus (ii) an out-of-band monitoring technology based on NetFlow summaries of packet flows:

Q. Did any part of the invention of the ’856 patent as far as you’re aware, did any part of the invention use NetFlow?

A. Without reading through the patent, I wouldn’t understand why it would and there was nothing brought up about using NetFlow that I know of.

* * * * *

Q. And the invention of the ’856 patent, the actual threat detection again was on a packet by packet basis inline, correct?

A. That was my understanding.

DTX-1685 at 140:5-10, 141:6-141:9.

Second, by the time a NetFlow record arrives at Stealthwatch (where ETA analysis occurs), the packets that are summarized by the NetFlow record have already “gone through the system” to their intended destination. Tr. 153:24-158:1, 1674:20-1676:2. It is thus impossible to “filter” or “route” them, as required by the claims, precisely because the out-of-band Stealthwatch device

never receives packets, but only receives NetFlow summary information about packet flows that were already delivered. At best, if Stealthwatch determines that NetFlow information corresponds to a threat, the administrator can act to address *future* packets. This fact cannot be debated; Cisco's fact witnesses, expert witnesses, technical documents, and source code are clear that Stealthwatch (and, by extension, CTA/ETA) only receives packet flow summaries (NetFlow) after the underlying packets are already delivered to their destination. Tr. 1672:19-1676:2, 2207:5-25. Even Centripetal's expert Dr. Cole agreed. Tr. 1066:2-6.

A third basis for non-infringement is that the claims require that whatever packets are "filtered" must then be routed to a "proxy system." Centripetal's infringement theory is that, if a network administrator reacts to the information provided by Stealthwatch (with CTA and ETA) by manually initiating a process whereby the ISE device issues a command for the routers and switches to quarantine the infected computer, then that quarantine command may cause future packets from that computer to be dropped. Tr. 1119:10-23. A router or switch drops packets by sending them to something called a "null interface," and that null interface is what Centripetal accuses as the required "proxy system," which is a requirement it had to add during prosecution to get the patent. Tr. 1095:9-12, 1097:3-12. But, far from a "proxy" (which stands in for something else) and far from a "system," a null interface is just a dead end; it is the mechanism by which dropped packets are eliminated. PTX-256; Tr. 965:2-6, 1853:24-1855:9. In contrast, the patent is clear that a "proxy system," as the name implies and as the Court found, must take an active role of "*interven[ing]* to prevent threats." Dkt. 202 at 21-22. Simply put, a null interface is neither a proxy for anything else nor a system that intervenes into anything.

D. The '806 Patent

1. The Requirements Of The '806 Patent's Claims

The '806 Patent addresses a specific way of swapping between sets of rules that are used

to filter traffic at inline devices, like gateways. As explained above, security devices (such as gateways) can filter packets using sets of rules, and they do so as the packets attempt to pass through the device. The rules are designed to identify harmful traffic; for example, based on the source of the packet. Each incoming packet is compared with the rules to determine if the packet triggers a rule, and then the rule may cause the packet to be dropped. Importantly, rules are changed periodically so that they stay up-to-date with current intelligence on network threats.

The '806 Patent references this background and focuses on the amount of time required for a device to switch rule sets: “[n]etwork protection devices may require time to switch between rule sets.” JTX-2 at 1:19-20. The patent explained that it is a problem to *keep using the old rules* while getting the new rules ready because the new rules might be needed to combat a network attack: “Additionally, while implementing a new rule set, a network protection device may continue processing packets in accordance with an outdated rule set.” *Id.* at 1:25-31.

The patent’s solution was as follows: send a signal to the gateway that packets should be processed with the new rules (*e.g.*, because of a network attack). Then, the claims require that “in response to” this signal, the device’s processor (which applies the rules to the packets) should “cease” processing all packets. Then, packets should be stored (“cached”) until the new rules are ready, at which time the cached packets should be processed with the new rules.

The specification explains each of these steps. First, the system stops processing packets when it determines that a rule set should be swapped. *Id.* at 7:35-43. Then, once the processor has ceased processing the packets, the packets on which the processing ceased, and any other incoming packets, are stored in a cache. *Id.* at 7:63-66. Then, once the new rules have been configured by the processor and are ready for use, the system’s processor resumes processing packets, beginning with the packets in the “cache.” *Id.* at 8:16-23. These requirements are set forth in the following

portion of the asserted claims (the “second rule set” is the new rules):

...signal, each processor of the at least two processors, to process packets in accordance with the second rule set; and
 configure, each processor of the at least two processors to, **responsive to being signaled to process packets in accordance with the second rule set:**
cease processing of one or more packets;
cache the one or more packets;
 reconfigure to process packets in accordance with the second rule set; ...
 responsive to receiving signaling that...[the] processors has completed reconfiguration to process packets in accordance with the second rule set, **process, in accordance with the second rule set, the one or more packets.**

Id. at 11:37-53 (claim 9); 10:48-64 (claim 17).

The prosecution history confirmed what Centripetal’s patent covers. The Patent Office rejected the claims as obvious in light of the prior art. Centripetal then amended its claims to add the requirements set forth above, including that, **responsive to** the signal to process packets with the second rule set, the processors “cease” processing packets and then “cache” those packets. DTX-1 at 1330-35; Tr. 2596:21-2598:20 (expert’s discussion of amendments to claims). Centripetal argued that the prior art cited by the Patent Office only showed that packets are stored in a “queue” (*i.e.*, a holding pen for data, also known as a “**buffer**”) while they wait their turn to be processed. By way of background, data or packets can arrive at a device (such as a computer) potentially faster than the device can process them. The multi-decade-old solution is to hold the arriving packets in a holding pen known as a “queue” or a “buffer.”

The packets are then processed from the buffer on what can be colloquially called a first-come-first-serve basis, or FIFO (“first in, first out”). Centripetal argued that the prior art “queue” was only configured “to hold packets for processing,” and is thus a “pre-processing queue that store[s] packets in a first-in, first out (FIFO) manner prior to processing” Dkt. 256, Ex. 5 at 13-14. Centripetal distinguished this prior art because a FIFO queue is not “configured to cache packets for which processing has ceased,” as required in the claims. *Id.* Centripetal was clear in its

comments to the Patent Office that conventional buffering of packets in a queue-while waiting for the processor to process them with a new rule set-is not what this patent covers. Instead, its invention was-in response to the signal that the system needs to use the new rule set-using a different memory (a cache) to hold the packets for which processing had stopped. *Id.*

This key difference is exactly what the claims recite. It is also exactly what Dr. Sean Moore, Centripetal's CTO and a named inventor of the '806 Patent, explained:

So in terms of technology, caching would be used in this sense, in this context, for, oh, those packets that you are currently processing through the old policy, **you don't want to like put those back on the buffer from whence you extracted them in the first place.** That's not a smart thing to do, number one. It would take some operations to pop those onto a buffer.

You want to put them in a higher-speed cache memory so that once you're ready to start processing those packets again, you can get to them as quickly as possible, minimize the – you know, the time that you're not providing service and making sure that you're securing those cache packets according to the new policy.

DTX 1688 at 167:21-168:10 (emphasis added).

2. The Difference Between The '806 Patent Claims And Cisco's Products

Centripetal's case reads as if it invented the basic concepts of switching between rule sets and using buffers as a holding pen for packets before processing them. Centripetal again proceeds as if the claims do not say what they say, the prosecution history never happened, the prior art does not exist, and its inventor had no idea what he invented.

Cisco's accused products operate in the manner that the patent described as the problem. JTX-2 at 1:25-31. After receiving a new rule set, Cisco's products continue to process packets from the buffer with the outdated rule set until the new rule set is ready for use, without ceasing processing or caching packets. Cisco does not view this as a problem, as its engineer explained:

Q. Okay. Do you have a view as to why it's okay for the Adaptive Security Appliance to continue to use the old rule set while the new rule set is being programmed?

A. That is correct. That's because it takes, you know, a human being, you know, several, typically hours or several – at least like a, you know, large amount of time to actually craft

these firewall rules, whether they're creating it from scratch or whether they're modifying them. And when they're ready to, say, push the button to allow them to take effect, **it's okay if it takes an extra few minutes for the firewall to fully program it before they take.**

Tr. 2518:22-2519:7. Using Cisco's accused switches as an example, those products process packets against a rule set at a specific cadence of one packet every 2- or 4- clock cycles (depending on the product), with each clock cycle being a billionth of a second (*i.e.*, a nanosecond). Routers also have a pre-set processing cadence. The processing cadence of a router or switch is never interrupted—let alone “ceased”—in any way, and certainly not *in response to* a signal relating to a new rule set. *Id.* at 2572:2-20 (Cisco engineer Peter Jones), 2619:4-2620:3 (Cisco expert Dr. Reddy). Instead, while a new rule set is being prepared for use by the router or switch, incoming packets continue to be processed with the old rule set, in accordance with the standard cadence. Then, when the new rule set is ready for use, a “pointer”—which is simply an indicator of which rule set the processor should use—switches to the new rule set instead of the old rule set. *Id.*; *see also* Tr. 2641:3-5 (Dr. Reddy: “the rules are swapped by merely storing your pointer, and the pointer now points to the new rule set.”). This swap happens during the natural idle period between the processing of any two successive packets. This idle time between any two packets always exists, regardless of whether the pointer swaps to a new rule set or not. *Id.* at 2572:2-20 (Jones). That standard idle time does not reflect a “ceasing” of processing, and it is not “responsive to” a signal regarding a new rule set. Likewise, nothing about the buffering of packets changes in response to a signal to swap rule sets—packets are put into and removed from a buffer the same way, regardless of whether a rule set is swapped during an idle period. Tr. 2563:7-19. Packets therefore are not “cached” as responsive to a signal regarding a new rule set.

Cisco's firewall engineer Hari Shankar explained that the other accused products operate in a similar fashion, in that the processing of packets is never interrupted—and certainly not “ceased”—due to a rule set switch. Instead, the switch to a new rule set is a “trivial” software

operation that happens between successive packets. Tr. 2518:4-13. The switch from using the old rule set to the new rule set has no effect on the buffer that all packets pass through while waiting to be processed. *Id.* at 2524:17-2525:11 (all packets received by the firewall are placed in a packet buffer “independent of whether rules are getting updated or not”). Thus, there is no “caching” of packets in response to a signal relating to a new rule set, as required by the claims.

VII. Centripetal’s Willfulness Case Relies On Unsupportable Copying Allegations

Cisco does not infringe, so Centripetal’s willfulness allegations fail. Centripetal’s willfulness case rests on its testimony that Cisco “look[ed] very suspicious,” Tr. 1031:3-10, and copying “could be plausible,” Tr. 3223:7-3224:3, because Cisco took meetings with Centripetal—the same premise it asserts against PAN. Centripetal never identified what exactly it disclosed that it alleges Cisco copied, nor who at Cisco did this copying. Centripetal never addresses the testimony from Cisco’s engineers, who developed the products, they did so years before these meetings, or the fact the engineers never interacted with Centripetal. Tr. 2531:1-10 (Shankar) (never heard of Centripetal before litigation), 2570:10-12 (Jones) (same); 1779:2-1780:23 (McGrew) (learned of Centripetal only in passing, never attended meetings with Centripetal).

The evidence instead shows that Centripetal repeatedly reached out to different people at Cisco to solicit investment. Centripetal made a high-level marketing presentation on its RuleGATE product and the use of “5 million+” rules to filter network traffic, instead of the standard rule sets of 10,000 rules—a technology Centripetal does not allege Cisco used. PTX-547 at 0193389. Almost all of the attendees testified there was nothing discussed at any level of technical detail. The one exception is Jonathan Rogers, Centripetal’s VP of Operations. Not only is his allegation self-interested—since he personally has hundreds of millions of dollars to gain—it is starkly inconsistent with the testimony of the other attendees. Even then, he concurred that no source code

or written algorithms were provided to Cisco. Tr. 1013:14-16, 1279:17-1281:16.

VIII. The Disconnect Between The Parties On Damages

Cisco does not infringe Centripetal's patents and thus owes no damages. Yet, to the extent the Court reaches the issue, Centripetal's damages theory has three significant flaws. First, damages must be tied to the specific acts of infringement, and the only possible acts of infringement are those instances where all accused components are combined. Centripetal nonetheless included within its royalty base the revenue associated with every sale of every component product. Using the '856 Patent as an example, the infringement theory only covers a router or switch *in combination* with Stealthwatch with ETA. But less than 100 Cisco customers (out of its 90,000+ customers for routers and switches) use ETA. Centripetal applies its royalty to all 90,000+ Cisco customers of routers and switches, even though the total number of customers with the allegedly infringing combination cannot exceed 100. Second, Centripetal failed to reliably identify the incremental value that its patents provide to the infringing combination. The Federal Circuit requires patentees to conduct an apportionment analysis that isolates the value of the patented improvement in the accused products. Centripetal's expert admitted to key failures in this analysis. Third, Centripetal's damages expert improperly relied on the licensing rate in a mid-trial settlement between Centripetal and one of its direct competitors (Keysight), without taking into account important technological and economic differences between that case and this one. In contrast, Cisco's damages expert determined the value of each patent based on (i) the extent of use of the actual accused combinations and (ii) the fact that most of the functionality in the accused products has nothing to do with the patents.

Dated: May 26, 2023

CISCO SYSTEMS, INC.

By: _____/s/_____
Of Counsel

Dabney J. Carr, IV, VSB No. 28679

TROUTMAN PEPPER

HAMILTON SANDERS LLP

P. O. Box 1122

Richmond, Virginia 23218-1122

Telephone: (804) 697-1200

Facsimile: (804) 697-1339

dabney.carr@troutman.com

Charles K. Seyfarth, VSB No. 44530

O'HAGAN MEYER

411 East Franklin Street, Suite 500

Richmond, Virginia 23219

Telephone: (804) 403-7137

Facsimile: (804) 237-0250

cseyfarth@ohaganmeyer.com

Louis N. Jameson (admitted pro hac vice)

Matthew C. Gaudet (admitted pro hac vice)

John R. Gibson, VSB No. 72968

Alice E. Snedeker (admitted pro hac vice)

DUANE MORRIS, LLP

1075 Peachtree Street, N.E., Suite 1700

Atlanta, Georgia 30309-3929

Telephone: (404) 253-6900

Facsimile: (404) 253-6901

wjameson@duanemorris.com

mcgaudet@duanemorris.com

jrgibson@duanemorris.com

jhforte@duanemorris.com

Joseph A. Powers (admitted pro hac vice)

DUANE MORRIS, LLP

30 South 17th Street

Philadelphia, PA 19103-4196

Telephone: (215) 979-1000

Facsimile: (215) 689-3797

japowers@duanemorris.com

John M. Baird, VSB No. 77827

Christopher J. Tyson, VSB No. 81553

DUANE MORRIS, LLP

505 9th Street, N.W., Suite 1000

Washington, DC 20004-2166

Telephone: (202) 776 7851

Facsimile: (202) 478 2620

cjtyson@duanemorris.com
Attorneys for Defendant
Cisco Systems, Inc.